UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

CHRISTOPHER HOLMES, *on behalf of himself and all similarly situated persons*,	:	
Plaintiff	:	
v.	:	Civil Action No. 3:22-cv-487
ELEPHANT INSURANCE COMPANY, ELEPHANT INSURANCE SERVICES, LLC and PLATINUM GENERAL AGENCY, INC. DBA APPARENT INSURANCE	:	JURY TRIAL DEMANDED
Defendants.	:	

CLASS ACTION COMPLAINT

Plaintiff Christopher Holmes ("Plaintiff"), individually and on behalf of all others similarly situated, bring this Class Action Complaint (the "Action") against Elephant Insurance Company, *a Virginia stock corporation*, Elephant Insurance Services, LLC, *a Virginia limited liability company which is a subsidiary, subdivision, or affiliate of Elephant Insurance Company*, and Platinum General Agency, Inc. dba Apparent Insurance, *a Texas corporation* (collectively, the "Defendants" or "Elephant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This Action arises out of the recent data breach at Elephant, an automobile insurance provider, that targeted the information of consumers who used or applied for insurance

services supplied by Defendants or Defendants' subsidiaries, subdivisions, or affiliates (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the Defendants' consumers' data. Because of the Data Breach, approximately 2,762,687 putative Class Members (including Plaintiff) suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack. In addition, Plaintiff and Class Members are now faced with the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their names, driver's license numbers, date of birth, and other sensitive information provided in connection with an insurance plan or application for an insurance plan (hereinafter, the "Personally Identifiable Information" or "PII").

3. As a result of the Data Breach, Plaintiff and Class Members have been harmed – they have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now guard against identity theft perpetrated using the stolen drivers' license numbers.

4. Plaintiff and Class Members may also incur out-of-pocket costs, for example, through having to purchase identity theft protection services, credit freezes, or other protective measures to deter and detect identity theft.

5. Plaintiff seeks to remedy those harms on behalf of himself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiff seeks remedies including, but not limited to, damages (inclusive of compensatory damages), reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendants' data security

systems and protocols, future annual audits, and adequate identity theft protection funded by the Defendants.

6. As such, Plaintiff brings this Action against Defendants seeking redress for its unlawful conduct, asserting claims for violations of the Driver's Privacy Protection Act, negligence, and negligence *per se*.

II. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act because (1) there are more than 100 putative Class Members, (2) the aggregate amount-in-controversy, exclusive of costs and interest, exceeds $5,000,000.00, and (3) there is minimal diversity because Plaintiff and Defendants Elephant Insurance Company are citizens of different states – namely, that Plaintiff is a Texas resident and the Defendants Elephant Insurance Company is a Virginia corporation, headquartered here in Virginia.

8. Alternatively, this Court has subject matter jurisdiction pursuant to 28 U.S.C. 1331 due to the Plaintiff's inclusion of claim alleged under the Drivers' Privacy Protection Act as well as supplemental jurisdiction over the state law claims alleged pursuant to 28 U.S.C. 1367, as all claims alleged herein arise from the same case or controversy.

9. This Court has personal jurisdiction over the Defendants because the Defendants are headquartered in this District. Additionally, this Court has personal jurisdiction over the Defendants because they have substantial contacts with this District and have purposely availed themselves to the Courts in this District.

10. In accordance with 28 U.S.C. 1391, venue is proper in this District because a substantial part of the conduct giving rise to the Plaintiff's claims occurred in this District, the

Defendants is headquartered in this District, and the Defendants transacts business within this District.

III. PARTIES

Plaintiff Christopher Holmes

11. Plaintiff Christopher Holmes is a resident and citizen of Big Springs, Texas.

12. Plaintiff Holmes received a letter dated June 3, 2022 from Defendants concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendants' networks. The compromised files contained full name and driver's license number, and may have also included date of birth, address, and any other sensitive PII provided in connection with an insurance plan or application.

The Elephant Defendants

Elephant Insurance Company

13. Defendants Elephant Insurance Company is a Virginia stock corporation with its principal place of business located in Henrico, Virginia. Elephant Insurance Company markets, sells and underwrites automobile insurance policies to consumers in Georgia, Illinois, Indiana, Maryland, Ohio, Tennessee, Texas and Virginia.

Elephant Insurance Services, LLC

14. Defendants Elephant Insurance Services, LLC is a Virginia limited liability company with its principal place of business located in Henrico, Virginia. Elephant Insurance Services LLC markets and sells automobile, homeowners, renters, motorcycle, and life insurance policies to consumers in Georgia, Illinois, Indiana, Maryland, Ohio, Tennessee, Texas and Virginia.

Platinum General Agency, Inc.

15. Defendants Platinum General Agency, Inc. dba Apparent Insurance is a corporation organized under the laws of the State of Texas, with a principle place of business at 9950 Mayland Dr, Ste 400, Henrico, VA 23233-1463. Defendants Platinum General Agency, Inc. is, upon information and belief, a wholly owned subsidiary of Elephant Insurance Company, and utilizes "Apparent Insurance" as a trade name.

IV. FACTUAL ALLEGATIONS

DEFENDANTS'S BUSINESS

16. Elephant Insurance, a subsidiary of Admiral Group plc. (a "U.K. leading insurer with a presence in eight countries and over 6 million customers worldwide"), is a "customer-centric" direct insurer.[1]

17. Elephant was founded in 2009 and is headquartered in Virginia.[2]

18. In order to provide insurance to consumers, Elephant collects a significant amount of private information, inclusive of the PII collected from Plaintiff and the Class Members. According to Defendants' "Elephant Insurance Privacy Notice," this information goes even beyond the scope of the information compromised in the Data Breach.

19. This information includes[3]:

a. Name;

b. Phone number;

c. E-Mail address;

d. Driver's license number;

e. Social Security number;

---

[1] https://www.elephant.com/about, (last accessed Jul. 11, 2022).
[2] *Id.*
[3] https://www.elephant.com/privacy, (last accessed Jul. 11, 2022).

f. Date of birth;

g. Marital status;

h. Vehicle information;

i. "information about other drivers";

j. Consumer report information ("information … obtain[ed] from third party consumer reporting agencies");

k. Transaction information (insurance policy information, claims history, billing and payment information); and

l. Website information (information obtained in part from cookies, such as "Internet Protocol (IP) address, operating system, and session ID").

20. All of this information, collectively, is extremely valuable.

21. On information and belief, in the course of collecting PII from consumers, including Plaintiff, Defendants promised to provide confidentiality and adequate security for customer data through their applicable privacy policy and through other disclosures.

22. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

23. Plaintiff and the Class Members reasonably relied (directly or indirectly) on this sophisticated company, with over six million consumers worldwide, to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Consumers, in general, demand security to safeguard their PII, especially when driver's license numbers and other sensitive PII is involved.

24. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

THE DATA BREACH

25. In June of 2022, Defendants first began notifying Class Members about a widespread data breach of its computer systems involving the sensitive PII of consumers. According to Defendants' Notice of Data Event (hereinafter, the "Notice"), the Data Breach occurred between March 26, 2022 and April 1, 2022.[4] The Data Breach was identified by Defendants at some point in April 2022 (Defendants does not say specifically); and, after a "comprehensive review" was conducted, on April 25, 2022, Defendants' "review identified the individuals whose information was in the affected data."[5]

26. The Notice also states the PII that was impacted: name, driver's license number, and date of birth.[6]

27. This Notice, which states in part that "Elephant Insurance… value[s] and respect[s] the privacy of your information," illuminates several issues: (1) Defendants are not truthful or transparent about when they discovered the Data Breach initially; (2) Defendants do not disclose how the Data Breach itself occurred; and (3) Defendants did not adequately monitor its systems, given the "unusual activity" on Defendants' network was not discovered until some point in April 2022, even though the intrusion began on March 26, 2022.

28. The Data Breach resulted in unauthorized access to the sensitive data of "Elephant Insurance customers or information [Elephant] received as part of providing a quote for auto or other insurance coverage." Because of the Data Breach, over 2.7 million Class Members' suffered

[4] https://www.elephant.com/notice-of-data-event, (last accessed Jul. 11, 2022).
[5] *Id.*
[6] *Id.*

ascertainable losses including out-of-pocket expenses and the value of their time incurred to mitigate the effects of the attack and the present and imminent harm caused by the compromise of their sensitive personal information.

29. The Personally Identifiable Information contained in the files accessed in the Data Breach was not encrypted.

30. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and the mutual understanding that Defendants would comply with its obligations to implement and utilize adequate data security measures to keep such information confidential and secure from unauthorized access. Defendants' data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach.

31. Therefore, the increase in such attacks, and the attendant risk of future attacks was widely known to the public and to anyone in the Defendants' industry, including the Defendants themselves.

THE DATA BREACH WAS FORESEEABLE

32. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry preceding the date of the breach.

33. Data breaches, especially those perpetrated against the insurance sector of the economy, have become increasingly widespread.

34. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[7]

[7] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed November 2, 2021)

35. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[8] Thus, Defendants' operation in the financial sector significantly, and predictably, increased its risk of being targeted by cyber criminals.

36. Cybercriminals were also becoming more effective. In 2019, financial sector data breaches exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[9]

37. Defendants were aware of the risk of data breaches because such breaches have dominatedthe headlines in recent years, including high-profile breaches for Equifax, Target, and various healthcare systems.[10]

38. In the first half of 2021, there were 846 data breaches in the country, on pace to set a new record. These data breach incidents impacted nearly 52.8 million individuals.[11]

39. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

---

[8] *Id*.
[9] *Id* at 15.
[10] *The 15 biggest data breaches of the 21st century*, CSO, Michel Hill and Dan Swinhoe, (July 16, 2021), available at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited July 11, 2022).
[11] https://www.idtheftcenter.org/post/data-breaches-are-up-38-percent-in-q2-2021-the-identity-theft-resource-center-predicts-a-new-all-time-high-by-years-end/ (last visited July 11, 2022).

40. Therefore, the universal increase in such attacks, and attendant high risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including, upon information and good faith belief, Defendants.

41. For these reasons, Defendants knew or should have known about these dangers and strengthened their data protection and computer system/network accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

DEFENDANTSS FAIL TO FOLLOW FTC GUIDELINES

42. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses to highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[12] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

---

[12] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016); *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 20, 2022).

[13] *Id.*

44. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

46. Defendants failed to properly implement basic data security practices.

47. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

48. Defendants were at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendants were also aware of the significant repercussions that would result from its failure to do so.

DEFENDANTS FAILED TO COMPLY WITH INDUSTRY STANDARDS

49. Several best practices have been identified that at a minimum should be implemented by companies like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

50. Other best cybersecurity practices that are standard in the Defendants' industry, and that upon information and belief Defendants did not employ, include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

51. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

52. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANTS' BREACH

53. Defendants breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard its computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

54. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its IT systems which contained unsecured and unencrypted PII.

55. Accordingly, as outlined below, Plaintiff and Class Members now face present and an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants.

HARM TO CONSUMERS

56. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

57. Specifically, driver's license numbers are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[14]

58. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your

[14] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021)

> driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[15]

59. According to cyber security specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[16] However, this is not the case. As cyber security experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[17]

60. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[18]

61. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a present and an increased risk of fraud and identity theft for many years into the future. Indeed, Plaintiff's driver's license number was found on the dark web following the Data Breach alleged herein.

---

[15] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021)

[16] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)

[17] *Id.*

[18] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

62. Thus, Plaintiff and Class Members must vigilantly guard against identity theft for many years to come.

63. Identity theft resulting from the Data Breach may not come to light for years.

64. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

65. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including driver's license numbers, and of the foreseeable consequences that would occur if Defendants' data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

66. Defendants knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

HARM TO PLAINTIFF

A. HARM TO PLAINTIFF CHRISTOPHER HOLMES

67. Plaintiff Christopher Holmes greatly values his privacy and PII. Prior to the Data Breach, Plaintiff Holmes took reasonable steps to maintain the confidentiality of his PII.

68. Plaintiff Holmes received a letter dated June 3, 2022 from Defendants concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendants' network from March 26, 2022 through April 1, 2022. The compromised files contained full names and driver's license number.

69. On or about June 21, 2022, Plaintiff Holmes received a notice from his identity theft protection service that his driver's license number was "found" on the "Dark Web."

70. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Holmes faces, Defendants offered him a 12 month subscription to a credit monitoring service. However, Plaintiff Holmes has not signed up for the program, as he does not trust that chosen vendor can protect his information. Moreover, traditional credit monitoring will not protect against the likely identity theft harm that will result from a compromised driver's license.

71. In mid-June 2022, Plaintiff Holmes began experiencing an uptick in spam text and telephone calls that he attributes to this Data Breach. Spam texts include unauthorized third-parties attempting to see Plaintiff Holmes insurance policies. Spam telephone calls include unauthorized third-parties posing as debt collectors attempting to collect fictional debts from Plaintiff Holmes.

72. Since learning of the Data Breach, Plaintiff Holmes has spent considerable time reviewing his bank statements and credit cards. Since receiving the Data Breach notice, he has spent approximately 5-10 hours reviewing his bank, credit and debit card statements. Moreover, Plaintiff Holmes spent this time at Defendants' direction. Indeed, in the notice letter Plaintiff Holmes received, Defendants directed him to spend time mitigating his losses by "reviewing your account statements and free credit reports for suspicious activity[.]"

73. The Data Breach has caused Plaintiff Holmes to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Defendants has not been forthright with information about the Data Breach.

74. Plaintiff Holmes plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

75. Additionally, Plaintiff Holmes is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

76. Plaintiff Holmes stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

77. Plaintiff Holmes has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

78. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Personally Identifiable Information was maintained on Defendants' system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class").

79. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

80. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 2.7 million individuals whose sensitive data was compromised in the Data Breach.

81. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personally Identifiable Information;

b. Whether the Defendants violated federal or state law with respect to the allegations made herein;

c. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

d. Whether Defendants' data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

e. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

f. Whether Defendants owed a duty to Class Members to safeguard their Personally Identifiable Information;

g. Whether Defendants breached a duty to Class Members to safeguard their Personally Identifiable Information;

h. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

i. Whether the Defendants knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendants' misconduct;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants violated the DPPA;

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

82. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

83. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

84. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

85. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

86. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

VIOLATION OF THE DRIVERS' PRIVACY PROTECTION ACT
(On Behalf of Plaintiff and the Class)

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

88. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

89. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

90. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(1). Drivers' license numbers are motor vehicle records and personal information under the DPPA.

91. Defendants obtain, use, disclose, resell, and redisclose motor vehicle records from their customers.

92. Defendants also obtain motor vehicle records directly from state agencies or through resellers who sell such records.

93. Defendants knowingly used motor vehicle records for uses not permitted by the statute, including sales, and marketing, among other impermissible uses.

94. Defendants knowingly failed to protect their computer systems and/or linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiff's and Class Members' PII, including the application website.

95. During the time period starting March 26, 2022, PII, including drivers' license numbers, of Plaintiff and Class Members, is available to thieves and has been removed from Defendants' computer systems. Defendants knowingly used and disclosed and/or redisclosed Plaintiff's and Class Members' motor vehicle records and PII to thieves, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

96. As a result of the Unauthorized Data Disclosure, Plaintiff and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

SECOND CAUSE OF ACTION

NEGLIGENCE
(On behalf of Plaintiff and the Class)

97. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

98. Defendants required Plaintiff and Class Members to submit non-public Personally Identifiable Information, including but not limited to their driver's licenses, as a condition of applying for or receiving insurance services from the Defendants.

99. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had and/or voluntarily undertook a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft.

100. Defendants' duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

101. Defendants also owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' information.

102. Only Defendants were in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach. Defendants breached their duty by failing to use reasonable measures to protect Plaintiff's and Class Members' Personally Identifiable Information.

103. The specific negligent acts and omissions committed by Defendants may include, but is not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Personally Identifiable Information (including but not limited to encrypting consumers' data);

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiff's and Class Members' Personally Identifiable Information; and

d. failing to recognize in a timely manner that Plaintiff's and other Class Members' Personally Identifiable Information had been compromised.

104. It was foreseeable that Defendants' failure to use reasonable measures to protect and monitor the security of Personally Identifiable Information would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

105. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

106. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendants' conduct constitutes negligence and awarding damages in an amount to be determined at trial.

THIRD CAUSE OF ACTION

NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Class)

107. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully alleged herein.

108. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

109. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

110. Defendants' duty to use reasonable security measures also arose under the DPPA, under which Elephant was required to protect the privacy, confidentiality, and integrity of driver's license information and only to use driver's license information in a permissible fashion.

111. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) along with the DPPA constitutes negligence *per se*.

112. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the DPPA, were intended to protect.

113. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the DPPA were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members. The DPPA was similarly enacted as a direct result of failures to protect consumer privacy like those outlined above.

114. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information

Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a

breach;

xiii. requiring Defendants to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

E. Ordering Defendants to pay for a lifetime of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages and compensatory damages, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

VIII. JURY TRIAL DEMAND

Jury trial is demanded by Plaintiff and members of the putative Class.

DATED: July 12, 2022

Respectfully submitted,

By: */s/Lee A. Floyd*

Lee A. Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (804) 351-9170
Lee@bbtrial.com
Justin@bbtrial.com

Jeffrey A. Breit, VSB #18876
Kevin Biniazan, VSB #92019
BREIT BINIAZAN, P.C.
Towne Pavilion Center II
600 22nd Street, Suite 402
Virginia Beach, Virginia 23451
Telephone: (757) 622-6000
Facsimile: (757) 670-3939
Jeffrey@bbtrial.com
Kevin@bbtrial.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877

dlietz@milberg.com

M. Anderson Berry*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

**pro hac vice forthcoming*